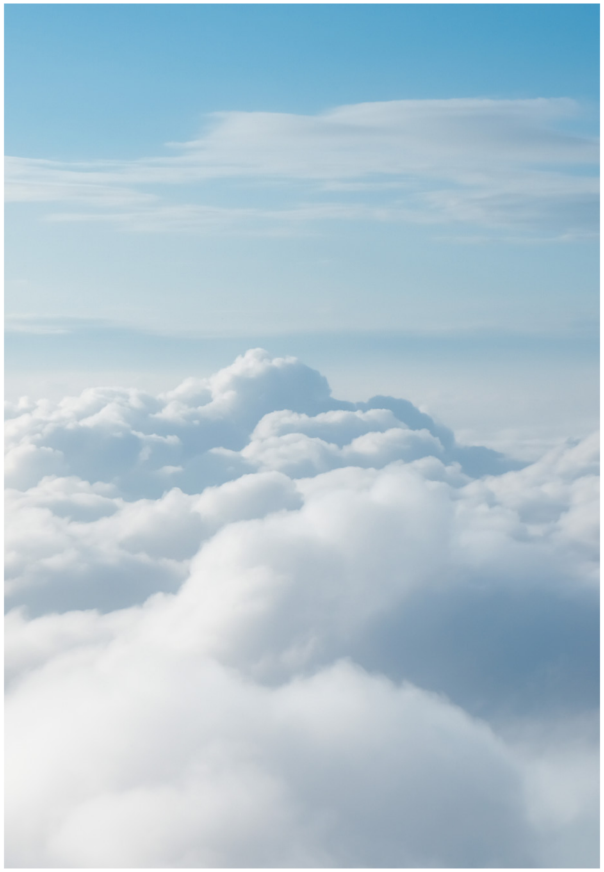
Commvault

eBOOK

RANSOMWARE 101

CONTENTS

TIME ACCELERATES IN A RANSOMWARE ATTACK



In the face of a ransomware attack, time is of the essence. Your vital business data is abruptly held hostage, encrypted by hackers who demand payment for its release. But there's a new twist to this threat - the use of AI. Hackers are leveraging advanced AI algorithms to enhance their attacks, making them more sophisticated and harder to detect. As you weigh your options, the safety of your data hangs in the balance. Refusing to pay may not guarantee its security, and even if you do pay, there are no guarantees. Meanwhile, your organization remains immobilized, with each passing minute intensifying the pressure to make the right decision.

This scenario has already struck companies of all sizes across industries worldwide.

Yours could be next.

ARE YOU READY?

WHAT IS RANSOMWARE PROTECTION?

The cyberthreat landscape, including ransomware, has transitioned to a case of when—not if. To ensure you can recover your data, you need the right solution with the best technology, the right people, and proven processes.

Cloud-based data protection solutions, powered by advanced AI and machine learning algorithms, provide robust protections against ransomware attacks. These solutions offer proactive monitoring and alerts, enabling organizations to promptly detect and respond to potential threats. Strong access controls, such as multi-factor authentication and role-based access, ensure that only authorized individuals can access critical data. Robust data encryption measures, both at rest and in transit, safeguard sensitive information from unauthorized access.

Additionally, comprehensive backup and recovery capabilities, including offline or air-gapped copies of data, enable organizations to quickly restore their systems and data in the event of a ransomware attack. By leveraging these cloud-based solutions and AI technologies, organizations can enhance their resilience against ransomware and effectively protect their critical data and recovery quickly.

Learn more >

By 2031, it is anticipated that ransomware attacks against businesses will occur

EVERY 2 SECONDS[1]

[1] Security Audit, Nivedita James Palatty, 100+ Ransomware Attack Statistics 2023: Trends & Cost, October 2023.

WHAT IS A RANSOMWARE ATTACK?

Gartner defines a ransomware attack as “cyber extortion where a malicious actor infiltrates an environment and encrypts and exfiltrates files, denying access and threating disclosure, unless the victim pays a ransom.”[2]

There’s a reason ransomware attacks make the headlines. They are sudden, brutal, often highly profitable, and leave the victim feeling helpless. In recent years, the rapid rise of ransomware has cast a shadow of anxiety across organizations. Alarmed businesses, IT staff, and security leaders aren’t just being paranoid.

A STAGGERING

72% OF BUSINESSES WORLDWIDE

have been affected by ransomware attacks this year. The average ransomware payment worldwide was over

$700,000.[3]

[2] Gartner, Gartner Glossary

[3] Statista, Ani Petrosyan, Business worldwide affected by Ransomware 2018-2013, October 2023 and Average amount of ransom payments related to cyber attacks Q1 2022- Q2 2023, September 2023.

TYPES OF CYBERATTACKS

It is easy to assume that all ransomware attacks are similar and that one size fits all in terms of prevention and preparation. However, because each type of ransomware is usually developed to infiltrate different, targeted networks, they can be very different in how they operate. Therefore, it is essential to understand the different types currently being used (keeping in mind that attackers are capable of combining multiple types of ransomware).

The strength of protection against any ransomware attack is in your defense strategy—especially given the rise in zero-day vectors with no known tactics, techniques, or procedures (TTP).

07 TYPES OF RANSOMWARE[4]

01 Locker ransomware can wreak havoc on a Windows systems. Victims may find a pop-up message on their screen with instructions such as, “Pay $100 fine to unlock your computer,” or “Click here to resolve the issue.”

02 Crypto ransomware is among the most common ransomware attacks available. It uses encryption to block access to files on a computer as well as any files stored or shared on network or cloud drives. Crypto ransomware is mostly spread through malicious emails, websites, and downloads.

Scareware uses fake security alerts to scare users into paying a ransom. This type of ransomware typically displays pop-up windows claiming there is an infection on the user’s computer and requiring payment.

03 Leakware is where attackers threaten to leak confidential information if the victim doesn’t pay the ransom. The hackers initially gain access to the system by exploiting vulnerabilities or social engineering techniques that allow them to steal the data.

04 Double extortion s a dangerous form of attack that not only denies access to data but also threatens its eventual public release should the ransom not be paid.

05 Triple extortion takes double extortion one step further by combining encryption, data exfiltration, and public shaming.

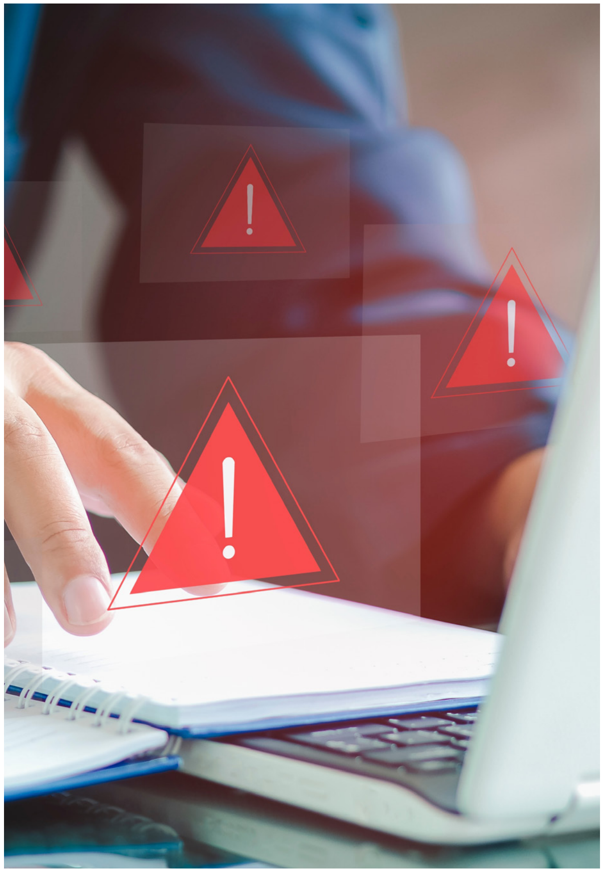
06 Ransomware as a Service (RaaS) is a cloud-based service that enables customers or “partners” to access and use ransomware with minimal technical knowledge or resources.

07 The RaaS model allows cybercriminals to run criminal ransomware enterprises without having to develop the code themselves, as they can outsource it from an existing provider.

Safeguarding against ransomware must be at the forefront of organizations’ security efforts.

[4] Enterprise Networking Planet, Kihara Kimachia, 7 Most Common Types of Ransdomware, with Examples, February 2023.

WHO ARE THESE BAD ACTORS?



External malicious actors are, in simple terms, villains. They are hackers or other individuals seeking to infiltrate your organization for their nefarious purposes. What are their motivations?

Some common motives may include:[5]

- Financial Gain: Many cybercriminals are motivated by financial gain.
- Espionage: Nations, states, and corporate competitors may engage to gather sensitive information.
- Hacktivism: Individuals or groups with political or social motives.
- Sabotage and Disruption: Some cybercriminals just want to disrupt critical infrastructure for political or ideological reasons.
- Personal Vendettas: Individuals may carry out cyberattacks due to personal grievances.
- Political Discord: Extremist groups may carry out attacks due to an ideological belief.
- And more...

Whatever their intention, they often use password-spraying techniques to gain unauthorized access to an organization or system. Or they might try to exploit vulnerabilities or inject botnets or rootkits to steal and delete data or disrupt an organization's ability to function.

That is where ransomware comes in. In a typical attack, the hacker uses malicious software (malware) to encrypt your data, often delivered via an infected attachment or link in an email. As in a flesh-and-blood ransom situation, the hacker then demands payment—or you'll never see your data again! Without an effective recovery strategy, you may think your only option is to pay the ransom and hope for the best.

[5] Sophos, Cybersecurity Explained, Threat Actors.

HOW DOES RANSOMWARE SPREAD?

Ransomware is most often spread through email phishing messages containing malicious links, unsecured public Wi-Fi networks, zero-day vulnerabilities, and, via drive-by downloading when a user unintentionally visits a contaminated site and malware downloads onto the user's computer or mobile device.

In any organization, the goal is to reduce risks and minimize the effects of ransomware. Commvault Cloud, powered by Metallic AI turns the tables on attackers, detecting ransomware sooner, accelerating recoverability, automating reporting and repetitive tasks, and assists in generating code actions and workflows to keep your data safe.

Ransomware protection does not have to be complex.

Protect your business from the ever-growing threat of ransomware with a robust and comprehensive cyber resilient plan. Commvault Cloud is purpose-built to cater to the specific requirements of hybrid enterprises, all while providing the lowest total cost of ownership. By leveraging the power of Commvault Cloud, you can effectively safeguard your valuable data, minimize the potential for data loss and exposure, and fortify your business against any future challenges that may arise.

10 TIPS TO MINIMIZE RANSOMWARE

01 **Regular Data Backups:** Ensures regular and automated backups of your critical data to reduce the impact of ransomware attacks, allowing you to restore your data to a previous, unaffected state.

02 **Immutable Data Storage:** Utilize immutable storage to prevent unauthorized modification or deletion of data, making it highly resistant to ransomware attacks.

03 **Advanced Threat Detection:** Employ advanced threat detection mechanisms to identify and mitigate potential ransomware threats before they can cause significant damage.

04 **Real-time Monitoring:** With real-time monitoring capabilities, detect any suspicious activities or anomalies in your data, enabling prompt action to prevent ransomware attacks.

05 **User Access Controls:** Establish robust user access controls, ensuring that only authorized individuals have the necessary permissions to access and modify critical data, reducing the risk of ransomware infiltration.

06 **Multi-factor Authentication:** Implementing multi-factor authentication adds an extra layer of security, making it harder for unauthorized individuals to gain access to your data and launch ransomware attacks.

07 **Encryption:** Employ strong encryption techniques to protect your data both in transit and at rest; make it extremely difficult for ransomware attackers to decipher and exploit your sensitive information.

08 **Security Patch Management:** Ensure you install regularly updates and patches its software and across SaaS apps to address any security vulnerabilities, minimizing the risk of ransomware attacks that exploit known weaknesses.

09 **Employee Training and Awareness:** Emphasize the importance of employee training and awareness regarding ransomware threats, equipping your staff with the knowledge and skills to identify and report potential risks.

10 **Incident Response Planning:** Develop comprehensive incident response plans, ensuring that your organization is well-prepared to handle ransomware attacks effectively and minimize their impact on your business operations.

HOW TO MITIGATE RANSOMWARE ATTACKS

When a ransomware attack occurs, organizations should take immediate steps to mitigate the impact and protect their data. The first crucial step is to isolate the affected systems from the network to prevent the malware from spreading further. It is essential to notify the appropriate authorities and engage with cybersecurity experts to investigate the attack and gather evidence.

Simultaneously, organizations should activate their incident response plan, which includes restoring data from secure backups, preferably stored offsite or in the cloud. Regularly updating and patching software, implementing strong access controls, and conducting employee training on cybersecurity best practices are vital protection measures. Organizations should also consider deploying advanced threat detection and prevention solutions, such as endpoint protection and network monitoring tools, to detect and block ransomware attacks in real-time. Regular data backups, encryption, and multi-factor authentication are additional layers of protection that can help safeguard against ransomware attacks.

Lastly, organizations should conduct post-incident analysis to identify vulnerabilities, improve security measures, and enhance their overall resilience against future attacks.

These steps provide the confidence that then an attack occurs, your backup data is protected and ready.

WHAT ARE THE RISKS OF PAYING THE RANSOM?

To pay or not to pay a ransom is a highly debated topic. Only you can decide what is best for your organization.

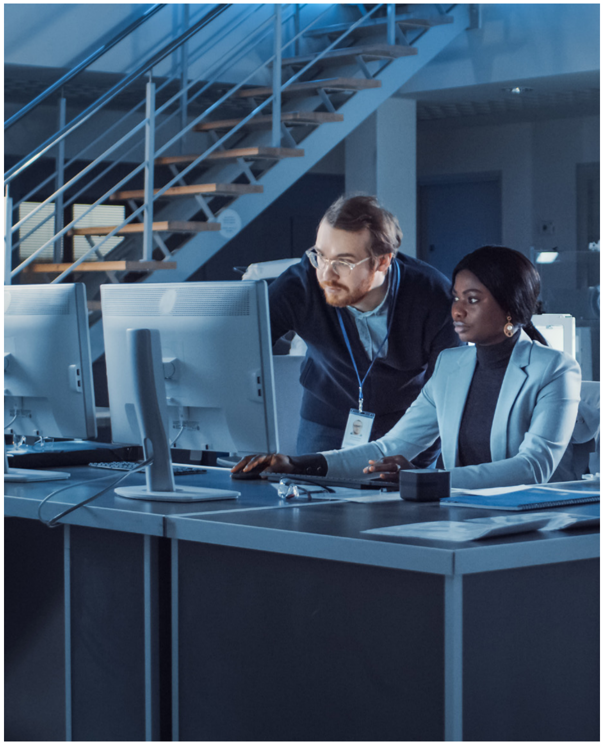
Paying the ransom in a ransomware attack carries significant risks and is generally discouraged by cybersecurity experts. While it may seem like a quick solution to regain access to encrypted data, there are several reasons why paying the ransom can be detrimental.[5]

- It encourages attackers.
- It escalates payments.
- Data isn't always returned. There's no guarantee attackers return the data or provide the decryption key.
- There could be future legal issues.

It is crucial for organizations to focus on prevention, backup and recovery strategies, and strengthening their cybersecurity defenses to mitigate the risks associated with ransomware attacks.

[5] TechTarget, Kyle Johnson, Should companies make ransomware payments?, August 2023

HOW COMMVAULT FIGHTS RANSOMWARE



Commvault Cloud, powered by Metallic AI, is the ultimate solution in the fight against ransomware and data protection. Our AI-powered solution employs intelligent algorithms and machine learning to detect and prevent attacks in real-time, ensuring the security of your valuable data. In the event of a ransomware attack, our solution provides cyber-resilient data protection with quick and efficient recovery. With secure offsite backups, advanced encryption, immutable backups, and cleanrooms, your data remains safe and accessible. Additionally, our solution offers comprehensive cyber resilience with features like multi-factor authentication and continuous vulnerability assessments.

Choose Commvault Cloud, powered by Metallic AI, for unrivaled data protection and resilience against evolving cyber threats. Trust in our advanced technology to keep your organization secure in the digital age.

CASE STUDIES

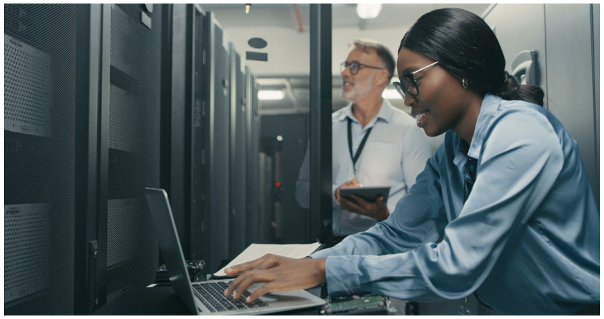
With Commvault Cloud, these organizations have been able to protect their data. The following case studies are just a few examples of how Commvault is helping organizations worldwide.

Delaware department of correction takes on ransomware

LEARN MORE

Harel Group simplifies its cloud journey with Commvault Cloud

LEARN MORE



Evolutio ensures data readiness and reduces costs with Commvault Cloud

LEARN MORE

DELAWARE DEPARTMENT OF CORRECTION TAKES ON RANSOMWARE

Established 1975

Background

Delaware Department of Correction (DOC) is a state agency that manages state prisons and maintains 24x7 mission-critical operations that provide healthcare, intelligence, video surveillance, secure movement, and safety. They collected personal healthcare information, medical records, rehabilitation, and release information and sought greater efficiency and security to manage and back up their data.

Challenge

DOC was looking to move away from paper backup to electronic data and build a resilient data management infrastructure to:

- Secure criminal, medical, and financial data for 4,500+ inmates across several facilities
- Specific data points such as video conferences, telephone calls, and footage from 2,000+ security cameras
- Mitigate the impact of a ransomware attack and create a data strategy that is future-proof

Solution

DOC implemented Commvault Cloud Autonomous Recovery to simplify backups and data storage across multiple facilities. Commvault protects all data, ensuring it is safe and highly accessible. After believing they had a data loss, Commvault quickly identified the problem, and DOC restored business operations within an hour.

Read the full case study

Responsive, 24x7 support services

60% cost reduction in tape media costs by moving to a more secure and reliable system

Scalable and resilient backup data architecture

Prepared for a ransomware attack

> **Commvault is the only vendor we trust to offer an all-in-one backup, disaster recovery, and ransomware protection solution.**

Phil Winder
Chief of Information Technology,
Delaware Department of Correction

HAREL GROUP SIMPLIFIES ITS CLOUD JOURNEY WITH COMMVAULT CLOUD

The Harel Group
PARTNERING FOR SUCCESS

Background

Harel Group is the largest and most innovative insurer in Israel, offering a wide range of products and services to over 10 million customers. With 80 years of experience in the industry, it is now listed on the Tel Aviv Stock Exchange and holds a 22% market share. They manage large volumes of data and investment money, so it is critical to ensure all data is backed up and restorable.

Challenge

Harel Group needed a single solution to protect data in the cloud and on-premises. They needed to ensure that data in the Microsoft Azure and Microsoft 365 cloud could be safeguarded and rapidly recovered as quickly and reliably as Commvault Cloud Autonomous Recovery protected their on-premises data.

Solution

Commvault Cloud Backup for Microsoft 365 was fast and easy, and implementing Commvault Cloud Air Gap Protect to drive on-premises storage to the cloud helped to minimize infrastructure costs and mitigate ransomware attacks.

Read the full case study

A total solution to ensure all data is 100% secure and can be restored at any time

Protected over 1,000 mailboxes with plans to scale over 5,000 mailboxes in a few month

Cut significant time in managing infrastructure for storage, media storage, and backup servers

> The combination of high security, ease of use, and fast deployment is the key factor for why Commvault won the race.
>
> **David Ben-Eli**
> System IT Infrastructure Manager, Harel Insurance

EVOLUTIO ENSURES DATA READINESS AND REDUCES COSTS WITH COMMVAULT CLOUD

evolutio

Background

Evolutio is a Madrid-based cloud services provider with over 30 years of experience. It has 6,100 virtual machines across three data centers and offers services to top Spanish organizations. Evolutio seeks to foster its customers' agility and innovation capacity and has used Commvault for ten years to protect its internal systems.

Challenge

The company sought an easy-to-use solution that consumed minimal resources to manage backup and security for Microsoft 365 with a desire to avoid yearly infrastructure upgrade costs and the ability to comply with regulatory requirements.

Solution

Installed Commvault Cloud Autonomous Recovery to backup and restore internal systems and expanded to Metallic® Backup for Microsoft 365 to protect 1,200 mailboxes and SharePoint.

Read the full case study

20% yearly savings in CAPEX

Ensure data is 100% secure

Installed Commvault Cloud in minutes

> Commvault Cloud is the pill you must take to get a good night's sleep. It gives us extreme confidence that our data is 100% secured.
>
> **Alain Rodriguez**
> Head of Services Management Office, Evolutio

eBOOK

CYBER RESILIENCE WITH COMMVAULT

Organizations need a redefined modern approach to cyber resilience with built-in security, defense, and rapid recovery – at the lowest TCO.

Learn more about how you can ensure cyber resilience at
commvault.com/use-cases/ransomware-and-cyber-defense

commvault.com | 888.746.3849 | get-info@commvault.com